

Program Notice

GIPSA PN-04-06

01/23/04

GIPSA ANNUAL SECURITY PLANS FOR INFORMATION TECHNOLOGY (IT) SYSTEMS AND SECURITY PROGRAMS

1. PURPOSE

This program notice establishes the Grain Inspection, Packers and Stockyards Administration (GIPSA) policy for the review and creation of IT security plans. This policy is a supplement to USDA, Office of Cyber Security Policy, **CS-025**, “Cyber Security Guidance Regarding Annual Security Plans for Information Technology (IT) Systems and Security Programs.”

2. EFFECTIVE DATE

This action is effective upon receipt.

3. BACKGROUND

Information security has escalated as the subject of high-level attention from both the press and media. Recent terrorist attacks have only highlighted the need to ensure that we have the highest level of information security practices. IT Security Plans have become the foundation document in the overall security process because they define the system security features and controls. They support Capital Planning and Investment Control (CPIC), Federal Information Security Management Act (FISMA) reporting, System Life Cycle efforts, Risk Management activities, as well as the Certification and Accreditation of Information Technology (IT) systems. Therefore, it is critical that they be prepared/updated on an ongoing basis with the most current information concerning each system's information security practices. These plans are submitted annually.

The Computer Security Act of 1987 and OMB A-130, Appendix III, require Annual Security Plans for IT Systems. Each plan should reflect accurate and comprehensive details required by NIST 800-18, Guide for Developing Security Plans for IT Systems. The generic term “system” covers all General Support Systems (GSS) and Major Applications. Security plans for other applications are not required because the security controls for these applications would be provided by the GSS in which they operate.

4. POLICY

The GIPSA IT Staff will develop and maintain an Overall Program Security Plan and individual Security Plans for all GSS and Major Applications.

These plans will be prepared using the instructions and templates for Overall Program Security Plan and individual Security Plans for all GSS and Major Applications available from USDA's Office of Cyber Security. These templates include a section to assist agencies in defining GSS and Major Applications and modified templates for electronic submission of plans. Modification of the templates closely parallels NIST 800-18 but also contains information required by FISMA and the Office of Inspector General audits. All security plans will be reviewed and formally approved by GIPSA's Chief Information Officer (CIO), Deputy Administrators, and Administrator prior to submission to the Office of Cyber Security.

All Security Plans will be due to the Office of Cyber Security each year by the last working day in April. The GIPSA Administrator must submit a cover letter with all plans attesting to the completeness and accuracy of the security plans. This letter will include information on whether the findings from the prior year's security plan submissions have been corrected or there is an Action Plan and Milestones in the FISMA Report. If the Office of Cyber Security does not require updated security plans, the most recent plans must still be reviewed and updated as necessary.

The USDA policy for IT security can be found at:
http://www.ocionet.usda.gov/ocio/cyber_sec/policy.html

5. QUESTIONS

Direct questions to the Information Systems Security Program at (202) 720-1741.

/s/ Donna Reifschneider

Donna Reifschneider
Administrator